PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: **WO 98/16033**

(43) International Publication Date: 16 April 1998 (16.04.98)

(21) International Application Number: PCT/US97/18164

(22) International Filing Date: 8 October 1997 (08.10.97)

(30) Priority Data:
08/731,186 10 October 1996 (10.10.96) US

(71) Applicant: PROTOCALL TECHNOLOGIES, INC. [US/US]; 47 Mall Drive, Commack, NY 11725–5717 (US).

(72) Inventors: BLUMENTHAL, Michael, S.; Apartment 1C, 560 Hew Highway, Hauppauge, NY 11738 (US). BARTHEL, Daniel, J.; 4423 Brygger Drive, Seattle, WA 98199 (US). NEWMAN, Bruce; 24 The Chase, St. James, NY 11780 (US). NEWMAN, Brenda, S.; 6 Doyle Court, Lake Grove, NY 11755 (US).

(74) Agent: GOLDMAN, Gregg, I.; Meltzer, Lippe, Goldstein, Wolf & Schlissel, P.C., 190 Willis Avenue, Mineola, NY 11501 (US).

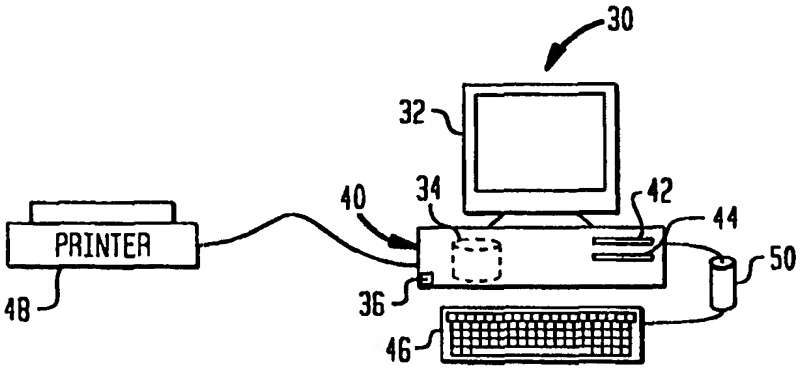
(81) Designated States: AU, BB, CN, CU, JP, KR, NZ, UA, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURED ELECTRONIC INFORMATION DELIVERY SYSTEM HAVING SEPARATE DATA MANAGEMENT

(57) Abstract

A system is provided for retrieving secured electronic information stored in at least one storage device (44), where each storage device, such as a CD–ROM, is at least partially encrypted and is coupled to a user station. Each user station (40) has a processor responsive to a data file system and to a separate application program. The data file system includes at least one database file, each comprising data corresponding to a respective software product. The processor that is responsive to the application product receives the data from the database file that corresponds to a user selected software product, requests (36) a decryption key from a remote network server based at least on the user selected software product data from the database files, and processes the requested decryption key that is selectively received from the server for decrypting the selected software product from the storage device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SECURED ELECTRONIC INFORMATION DELIVERY SYSTEM HAVING SEPARATE DATA MANAGEMENT

Related Applications

U.S. Patent Application Serial Number 08/731,185, entitled "Secured Electronic Information Delivery System Having a Metering Device," was filed on October 11, 1996 for Daniel J. Barthel et al. and U.S. Patent Application Serial Number 08/720,968, entitled "Secured Electronic Information Delivery System Having a Three-Tier Structure," was filed on October 11, 1996 for Daniel J. Barthel et al. The above-noted applications are assigned to the assignee of this application. The contents of the above-noted applications are relevant to the subject matter of this application and are fully incorporated herein by reference.

Field of the Invention

The invention relates generally to a system for retrieving secured data from a storage device and, more particularly, to a system having a user station with a data file system separate from an application program for selectively receiving decryption keyes from a remote server to retrieve secured data from a storage device.

Background of the Invention

Traditional methods of product distribution within the retail software business generally involve the retailer having to purchase up-front inventories of each product before actual market demand can be determined. Moreover, retailers inevitably face the "80/20" rule - unless you have the 80% of

inventory in stock which rarely sells, you won't have the opportunity to sell the 20% which does sell frequently. The only alternative previously available to retailers was to arrange a consignment inventory with the supplier. Consignment, however, does not resolve "out-of-stock" items, space requirements, or inventory management issues. Consignment inventory also bears a large up-front cost for suppliers.

These factors, combined with increased competition from superstores, declining retail prices, and the perceived threat of the Internet as a convenient mechanism to purchase a wide assortment of software products, make traditional methods of software distribution highly inefficient in today's market environment. Therefore, there is a need for retailers to be able to produce software products "on-demand" as the items are needed. One such solution is a system for retrieving secured data from a storage device.

In a conventional system for retrieving secured data from a storage device, the storage device may be located remotely from the retailer's user station over, e.g., a local area network (LAN) or a wide area network (WAN) or be located at the user station from, e.g., a CD-ROM.

In systems where the storage device is at the user station, the user's access to the secured data from the storage device needs to be regulated. For example, in a hardware based system developed by Infosafe Systems, Inc., such regulation is accomplished by a metering chip that comprises all of the decryption keys to unlock the desired secured data from a CD-ROM. Essentially, a SCSI (small computer system interface) device, acting as an external hard drive and connected to the user station, includes the metering

chip having the decryption keys. The selected secured data is decrypted with a corresponding decryption key, while the user's order is simultaneously written and stored in the flash memory of the SCSI device. However, for the distributor to monitor each user station's usage (for billing purposes), every user station must be polled on a regular bases, e.g., daily, to capture the data stored in each SCSI device and subsequently purge the flash memory. This system has the disadvantage in that the distributor must poll each user station having the metering chip which is extremely time consuming, if not unrealistic, when the amount of user stations are in the thousands.

In another hardware based system by Wave Systems Corp., another metering chip that comprises all of the decryption keys to unlock the desired secured data from a CD-ROM has been developed. However, unlike the system by Infosafe, the metering chip is not located in an external SCSI device but in the motherboard of the user station. This system has the same disadvantage in that the distributor must poll each user station having the metering chip. Further, any PC or Macintosh based user station would require that the motherboard be manufactured with the metering chip. This has the inherent disadvantages of taking up valuable real estate, i.e. space, on the motherboard, adding a significant cost to new computers, and difficult to service if there is a problem with the chip.

In another secured data delivery system, developed by the assignee of this application, a combined hardware and software system has been produced. In this system, a retailer is supplied with a CD-ROM having encrypted software products stored thereon, and an application program (hereinafter an

"Application") including the product information corresponding to the encrypted software products and a decryption algorithm capable of taking partial decryption keys, supplied transparently from a remote server, to generate corresponding full decryption keys to decrypt the selected software products from the CD-ROM.

However, in this system, since product data information is encrypted and incorporated into the Application program, a new Application is needed any time there is a change to the available products or when additional products or manufacturers are offered. Further, the Application risks becoming "bloated" with data and would require more memory to run as the number of products and manufacturers increases with time. Additionally, this system does not contemplate having a retailer sell CD-ROMs and Application software to customers, while being able to monitor the consumer's use by having the user connect to the retailer for decryption keys. Furthermore, this system requires that the retailer contact the server to receive the decryption keys every time the retailer produces a software product.

It is therefore an object of the present invention to overcome the disadvantages of the prior art.

Summary of the Invention

This and other objects are realized by an inventive system and method of retrieving secured electronic information stored in at least one storage device, where each storage device is at least partially encrypted and is coupled

to a user station. The user station may be used by a retailer, a consumer, and the like.

In one embodiment, each user station is coupled to at least one storage device, such as a CD-ROM. Each station has a processor responsive to a data file system and to a separate Application program. The data file system includes at least one database file, each comprising data corresponding to a respective software product.

The processor, responsive to the Application program, receives the data from the database file that corresponds to a user selected software product, requests a decryption key from a remote network server based at least on the user selected software product data from the database files, and processes the requested decryption key that is selectively received from the server for decrypting the selected software product from the storage device.

In another embodiment, an end-user station is coupled to at least one storage device, such as a CD-ROM, where each station has unique serial number and a processor that is responsive to an Application program stored therein. The user can select a software product to decrypt upon receipt of a corresponding decryption key.

A remote vendor station, having a unique password, is selectively coupled to the end-user station, via a network, to receive a request for the decryption key corresponding to the selected software product. Further, the vendor station receives the serial number from the end-user station.

A remote server is connected to the vendor station, via a network, when the password transmitted from the vendor station is validated. The server receives a request for the decryption key corresponding to the transmitted selected software product and the end-user serial number. The server then generates and transmits the decryption key to the vendor station based on the selected software product and the serial number. Thereafter, the vendor station transmits the decryption key to the end-user station, so that the end-user Application program can decrypt the selected software product based on the received decryption key.

In yet another embodiment, each user station (vendor or consumer) is coupled to at least one storage device, such as a CD-ROM, having at least one electronic database file stored therein. At least one of the database files stores numerous decryption keys, each key corresponding to decrypting a predetermined data portion of the secured electronic information.

Further, a metering device is coupled to each user station. When the metering device is valid, each respective user station is able to retrieve decryption keys from the corresponding database file for use in decrypting the corresponding selected data portion. In addition, a server that is selectably connected to each user station across a network controls whether the metering device is valid and operable so as to permit or deny the user station to retrieve the corresponding decryption keys.

Brief Description of the Drawing

The following detailed description, given by way of example and not intended to limit the present invention solely thereto, will best be understood in conjunction with the accompanying drawings in which:

FIG 1 is a diagram schematically illustrating a three-tier network having a server connected to a first group of user stations, where a station in the first group is connected to a second group of user stations, in accordance with the present invention.

FIG 2 shows an example of a user station of FIG 1, in accordance with the present invention.

FIGs 3A-3D is a flow chart showing the steps for decrypting selected software products from one of a plurality of CD-ROMs connected to a user station from the first group of stations, in accordance with the present invention.

FIGs 4A-4D is a flow chart showing the steps for decrypting selected software products from one of a plurality of CD-ROMs connected to a user station from the second group of stations, in accordance with the present invention.

FIGs 5A-5D is a flow chart showing the steps for decrypting selected software products from one of a plurality of CD-ROMs connected to a user station from the first group of stations having a metering device, in accordance with the present invention.

Detailed Description of the Inv ntion

The preferred embodiments of the present invention all relate to a system where a retailer or a consumer may access software products from a storage device, such as a CD-ROM, that is coupled to the retailer or consumer user station or computer. Each software product on, e.g., a CD-ROM, has been secured by an encryption technique so that the retailer or consumer may access any encrypted software product upon receipt of a decryption key.

For example, in one embodiment, every time the retailer or consumer wants to decrypt a software product, the retailer or consumer user station must link up with a remote server. The server will first ascertain that the station may access such decryption keys through, e.g., passwords and external serial numbers. Once the connection is validated, the server may generate the desired decryption key, based on, e.g., the software product item number, an internal serial number (not known to the retailer or consumer) and a purchase code.

For added security, the decryption key generated by the server is preferably only a partial decryption key. Thus, if the decryption key required to unlock an encrypted product is 56 bits long, a partial key may simply be a portion thereof. The retailer or consumer user station, having an Application program, generates the full 56 bit decryption key. If the station is a retailer station, the retailer typically will decrypt and write a product onto an end-user media of choice, such as a floppy disk.

In another embodiment, the retailer or consumer user station has a metering device or "dongle" attached thereto for monitoring and selectively preventing access to decryption keys that are stored, not in a remote server, but in a known path to the Application in each station. In this case, the dongle will only permit a predetermined amount of products to be decrypted, an unlimited amount of products but for a predetermined amount of time, a predetermined monetary amount, or any other preset criteria. Once the preset criteria has expired, the retailer or consumer must link up with the remote server for revalidation.

As seen in FIG 1, a network 10 is illustrated having a server 15 that may be directly connected to a plurality of stations 16, 17, 18, 19 and 20 of first station group 12. Server 15 may be a conventional computer having PC DOS or Windows®, Macintosh®, UNIX or other OS (operating system) platform or a specialized server such as an exemplary Sun® Server. Server 15 may be connected to any station in station group 12, and vice-versa, by, for example, a typical modem link or LAN/WAN connection. A station may also be a conventional computer having any platform. Although only five stations in station group 12 are shown, it should be understood that there is substantially no limit to the amount of stations connected to server 15.

FIG 1 also shows a second station group 14 that includes stations 24, 25, 26, 27 and 28. As with station group 12, additional stations can be added to group 14. As shown, station 17 may be connected to each station in group 14. Additionally, every station in first station group 12 may be connected to stations in second station group 14 or other station groups (not shown).

Further, stations from the first station group may communicate with stations from the second station group, and vice versa, without being physically connected via a modem link or LAN, but by facsimile machines and the like, external to each station.

As stated, stations 16-20 and 24-28 are typical computer systems, preferably PC or Macintosh® based. FIG 2 illustrates a conventional computer station which includes a computer housing 40, a monitor 32 and a keyboard 46. Housing 40 comprises a modem jack 36, a hard drive 34, a floppy disk drive 42 and a CD-ROM drive 44. Of course, a station may include additional or less hardware as desired. Connecting housing 40 with keyboard 46 is a metering device or dongle 50 which, as will be described hereinlater, may prevent a station user from decrypting secured data from a storage device, such as a CD-ROM. It should be noted that the dongle may be connected to any external or internal station port (not shown), as well. A printer 48 may also be included for printing out, among other things, software manuals and disk labels.

Prior to decrypting any software products, each station preferably has specialized software for installing an Application program and a data file system, such as a directory, although the directory may be included in the Application program, if desired. The directory includes separate database or resource files and universal files. In short, the database/resource files include each software manufacturers or foundries name and corresponding software product name, so that when the Application program is launched, the station will dynamically build menus that include each manufacturer and a list of each corresponding software product. Further, the database files include trademark

information for each manufacturer, and the correct path for each software product, i.e. on which CD-ROM. Since the database files are preferably separate from the Application program (although the Application program retrieves the data from the database files), it is relatively easy to upgrade or limit the amount of manufacturers available on each station.

The universal files in the directory link together necessary products that are required for each selected manufacturer product. For example, if a user selects a software product from a specific manufacturer, three additional products may need to be retrieved for the selected product to work. Also, depending on the platform of the station (PC, Macintosh, etc.) certain programs must be linked with the selected product. For example, if the station has a Macintosh platform and requires a specific utility to run the selected software product.

The Application program performs the majority of the functions for the station when decrypting software products. Among its functions are dynamically building manufacturer and software item menus, linking with the server or other stations, generating full decryption keys from partial keys, accessing the selected software product from one of a plurality of CD-ROMs, performing the decryption algorithms of the selected products for storage on, e.g. the hard drive or a floppy disk (or any high density storage medium), and queuing an attached printer to print out software manuals, labels for the floppy disks, and the like.

The software products, stored on the CD-ROMs, are preferably encrypted in the following manner. Each unsecured product is first encrypted by a conventional encrypting process using a unique corresponding encryption key. Thereafter, each encrypted product is decrypted using a unique phantom key. A phantom key is any random key so long as it is not the same as the unique encryption key. Each phantom decrypted product is then written to a corresponding CD-ROM. This scheme of first encrypting and then decrypting with a phantom key ensures that the software products on the CD-ROMs are virtually unbreakable without having both the phantom key and the encryption key. It has been estimated that it would take a Cray supercomputer approximately five years of non-stop processing to break the key codes for each software product. Of course, any encryption scheme will work with this invention as well.

FIGs 3A-D is a flow chart showing the steps for decrypting selected software products from a plurality of CD-ROMs from a retailer or consumer station (in station group 12), where a partial decryption key, for each selected product, is generated from the remote server.

At step 60, the retailer or consumer user station is powered on and the Application program is launched. For example, on a Windows based operating system, the user would "click-on" the Application icon. At step 62, once the Application is launched, it checks that all of the necessary files from the directory are present. If not, an error message is flashed on the monitor and, upon user confirmation, the Application is terminated at step 64. Assuming that all files are present, at step 66, the Application will read the available

database files and include the contents of these files in dynamically built menus. An example of a dynamically built menu would be a list of manufacturer and corresponding product menus.

At step 68, the station is idle while it waits for a user input. At step 70, the user will select the software product item or items that need to be decrypted and optionally written on a storage device. The user may select the desired item via SKU numbers, actual product names, scrolling lists or other criteria depending on the product. At step 72, the Application searches in the database files for the selected item. If, however, the item was selected from a scrolling list (a list created from the menus built from the database files), then the user selected an item directly from the database and therefore, a search is not necessary. Step 74 indicates that the selected items were found. If not, step 76 will alert the user and return to step 70.

Assuming that the item is found, the selected item will be added to an Order Detail screen that includes other selected items, if any, at step 78. In the Order Detail screen, the user can select some or all of the selected items for decrypting and manufacture. Step 80 inquires if the user wants to select more product items. If yes, then the user returns to step 72, while if no, the user initiates the request for decryption keys to decrypt each selected item, at step 82, by, e.g., clicking a Request icon.

At step 84, a registration data entry screen that includes a space to enter in the customer's name, address, and the like appears. This feature enables the retailer or the consumer himself to register the user of the selected software product with the manufacturer, so that the user can receive additional

information regarding updates, etc. Further, this enables the retailer to build a customer database of software purchasers simultaneously. At step 86, the Application ensures that all fields in the registration data entry are populated. If not, the user optionally is returned to step 84.

At step 88, the Application will request the station user's name and a pre-assigned password which will be subsequently transmitted to the server at step 90. At this step, the Application will preferably automatically dial a predetermined phone number to connect to the remote server. To avoid anticipated traffic of several stations trying to connect to the server simultaneously, conventional network solutions can be implemented if a server is on a LAN.

At step 92, in the event of a busy signal, the Application will continue dialing periodically until a connection is made or the user terminates the process. At step 94, connection to the server is made. At step 96, the server will initiate a series of requests for data to determine if the station is qualified to "Login" to the server. Some of the criteria include the station name, a password, and the external serial number. At step 98, if access to the server is denied, the modem connection is terminated by, e.g., an ATF command, at step 100. If access is granted, step 102 transfers the Order Detail and registration data entry information to the server. The server may store this information for future billing and royalty reporting purposes. Further, in this step, the product item number, the external serial number, and a purchase code, among others, is supplied to the server. The purchase code is a code generated by the Application that is not dependent on the selected product item

but based on the internal serial number of the Application. Based upon the supplied information, the server generates partial decryption keys to be transmitted to the requesting station.

At step 104, the partial decryption keys are transmitted transparently to the Application via the modem. This partial decryption key is invisible to the user and is only used internally to generate the full decryption keys in step 106. At step 106, the Application generates the full decryption keys that will decrypt the selected software product. This is achieved, e.g., by using a private key encryption/decryption scheme. The full decryption keys are preferably 56 bit keys using the multi-level encryption scheme previously discussed. For example, since only portions of the decryption keys are sent, there is little risk of a security breach since the balance of the decryption key that needs to be used is calculated "on-the-fly" by the Application.

At step 108, the Application queries whether there are any items to print. That is, if the product requires labels or documentation, the Application will generate these documents locally at the station's printer. The labels are for the floppy disks and casing which will be manufactured, if desired, for the decrypted software products. The labels and documentation may or may not be encrypted in the database or CD-ROM, depending on the manufacturer's specifications. If there are items to print, the printing routines are initialized at step 110. Once the items are printed, the user will have the opportunity to check the documents for printing flaws, at step 112, and if necessary reprint the documentation back at step 110. If the documentation is error free, or if the user chooses not to print any items, the encrypted CD-ROM volume is

determined at step 114. The path to the correct CD-ROM that contains the selected encrypted product is stored in the corresponding database file. Preferably, a dialog box will appear requesting that the user mounts the appropriate CD-ROM for the item or items that need processing. In the event that the order contains items that are located on multiple CD-ROMs, the Application will process the first item, then request that a new CD-ROM be mounted, and proceed with processing that item.

At step 116, the Application checks to make sure that the CD-ROM mounted is the correct one. If not, at step 118 the Application requests for the correct CD-ROM and at step 120, the user may change to the correct CD-ROM. If it is still not correct, the process returns to step 118; however, if the CD-ROM is now correct the process proceeds to step 122 where it is determined whether the selected item is found on the corrected CD-ROM. If not, the CD-ROM is likely outdated and an error message will appear which terminates the order.

Once the item is found, the process proceeds to step 126 where the full generated decryption keys are used to decrypt the selected items from the Order Detail. These keys are then immediately discarded by the Application and thus cannot be used again. This occurs since the keys that are generated may only exist one time for a single order. The keys that are generated in the future to decrypt the same item will be completely different. Thus, the full decryption keys are only temporarily stored in a RAM (random access memory) until the item is decrypted and then discarded. At step 128, the decrypted items are checked by the Application in a process called "CheckSum" to insure the

integrity of the data. In the event of a CheckSum error, the order will be terminated at step 130. In this case, it is most likely that the internal serial number in the Application has been set incorrectly or that the installation procedures were not correctly followed.

At this point, the selected product item has been decrypted and is temporarily stored in the station memory. If the station user is a consumer, the product may be stored on the hard drive of the station. Alternatively or in addition to, the consumer may also write the decrypted product to a blank floppy disk. On the other hand, if the user station is from a retailer, the product may only be stored temporarily in the RAM as was the decryption key. At step 132, the Application will request a media type to be mounted. Preferably, the media is a floppy disk which is specially serialized. If the Application requires that the floppy disks be specially serialized, then the specialized disks must be supplied to the user since no other media will work with the system. This procedure is to ensure quality control and maintain a control over the amount of products that can be decrypted per retailer and consumer station.

At step 134, the Application determines whether the media are the correct type and formatted for the correct platform. Additionally, the Application "flags" the media once it is mounted so it cannot be used again. If the media does not meet these criteria, the media will be rejected, and a request will be made of the user to mount valid media back at step 132. Assuming that the media is correct, the product items are copied to the media at step 136.

At step 138, the Application determines whether the media is filled to capacity or require decryption from multiple CD-ROMs. If the order is not complete, the process is returned to step 132. If the order is complete, the Application will return to the Order Detail screen at step 140. At step 144, the order screen is cleared and the Application is ready for the next order to be processed through the system. At step 146, the station is idle waiting for the user to initiate the next selected item, if any. Lastly, at step 148, the process is ended.

FIGS 4A-D is a flow chart showing the steps for a consumer decrypting selected software products from a plurality of CD-ROMs from the consumer station. In this embodiment, the consumer preferably goes through the retailer, where the consumer purchased the software and CD-ROMs, to receive the partial decryption keys, as desired. The retailer, in turn, connects to the server for the partial decryption keys and once received, subsequently transmits on line or by facsimile to the consumer.

Steps 300 to 320 are essentially identical to steps 60 to 80 of FIG 3A and therefore will not be redescribed. At step 322, the consumer user will contact the retailer, where he purchased the Application program, for the partial decryption keys. The user may contact the retailer by telephone or facsimile to request the partial decryption key for the selected software product, or may contact the retailer via other networks, such as a modem. The information supplied to the retailer include the product item number, the purchase number and an external serial number that was supplied with the Application program.

At step 324, the retailer initiates a request for the partial decryption keys from the remote s rver.

Steps 326 to 340 are substantially the same as steps 84 to 94 and 102 to 104 of Figs 3A-B, and therefore will not be redescribed. At step 342, the retailer transmits by modem, facsimile or telephone a partial decryption key, which is preferably 9 bits in length. At step 344, the consumer user enters the 9 bit partial decryption key into the Application to internally generate the full 56 bit decryption key to decrypt the selected product item.

Steps 346 to 368 are essentially the same as steps 108 to 130 of FIG 3C and therefore will not be redescribed. At step 370, the Application preferably moves the decrypted software product from the CD-ROM to the recepticle directory. If a directory path is not located, an error message will flash so that the user may create a proper directory at step 372. At step 374, the decrypted product items are copied to the directory on the consumer's hard drive. Steps 376 to 382 are essentially the same as steps 140 to 148 of FIG 3D, and therefore, will not be described.

FIGS 5A-D is a flow chart showing the steps for decrypting selected software products from a plurality of CD-ROMs from a retailer or consumer station (in station group 12), where the partial decryption keys are generated from the station itself. In this embodiment, a dongle 50 is utilized to monitor the amount of items decrypted, as previously described. The partial decryption keys are located in a "resource" file which is one of the database files in the directory.

Steps 200 to 206 are essentially the same as steps 60 to 66 of FIG 3A and therefore will not be redescribed. At step 208, the Application verifies that it is set to require a hardware dongle. Further, the Application checks that there is an resource file. If the Application is not set to receive the dongle or if the resource file is not present, then at step 210, the process may proceed to step 68 of FIGS 3A-D, or else terminate.

At step 212, the Application verifies that the bus, preferably a Processor Direct Bus, is connected to the dongle. At step 214, if there is no dongle, an error message is generated and the Application is flagged or terminated, at step 216. At step 218, the Application verifies that the dongle is set specifically for the Application. At step 220, an error message is generated and the Application is terminated if the dongle failed the verification.

At step 222, a dialog box appears on the monitor informing the user that the dongle has an expiration date approaching in X number of days, in X number of additional manufacturing sessions, by X number of dollars, and/or any other criteria, as desired. At step 224, if either limits are expiring, the user can initiate a revalidation process at step 226. Preferably, the dongle is revalidated on line by the remote server at the server's discretion at step 228. Once the dongle is revalidated the process returns to step 200 and the user may begin again.

If the use limit was not running out or expired, at step 230 the user may determine that it is premature to initiate the revalidation process and instead elects to proceed with the manufacturing process.

Steps 232 to 252 are essentially the same as steps 68 to 88 of FIGS 3A-B and therefore will not be redescribed. Additionally, steps 254-258 are essentially the same as steps 96-100 of FIG 3B and will also not be redescribed.

At step 260, in the event that access is granted, the order detail and the customer's registration information will be written to a preferably DES encrypted database file where it will be stored for future billing and royalty reporting purposes. For example, every time that the user goes on line with the server to revalidate the dongle (at step 228) the server will automatically retrieve the data from the DES resource file. At step 262, the partial decryption keys are retrieved from the resource file. At step 264, the dongle is updated indicating that an additional use has procured.

Steps 266 to the end at step 299 are essentially the same as steps 106 to 144 of Figs 3B-D and therefore will not be redescribed.

While several embodiments have been chosen to illustrate the invention, it will be understood by those skilled in the art that various changes and modifications can be made herein without departing from the scope of the invention as defined in the appended claims.

Claims

The claimed invention is:

1. A system for retrieving a plurality of secured electronic information stored in at least one storage device, each being at least partially encrypted, and each of said plurality of secured electronic information being a software product, comprising:

at least one user station coupled to said at least one storage device, each having a processor responsive to a data file system and to a separate application program stored in said user station,

said data file system including at least one database file, each comprising data corresponding to a respective one of said plurality of software products,

wherein said processor, responsive to said application program,

receives said data from said database file that corresponds to a user selected software product,

requests a decryption key from a remote network server based at least on the user selected software product data from said database files, and

processes the requested decryption key, selectively received from said server, for decrypting said selected software product from said at least one storage device.

2. The system of claim 1, wherein each said decryption key that is requested and processed by said processor, responsive to said application program, is a partial decryption key, and wherein said processor generates a

corresponding full decryption key, for decrypting said selected software product from said at least one storage device, based on said partial decryption key.

3. The system of claim 2, wherein said generated full decryption key is stored in said user station only until said selected software product is decrypted.

4. The system of claim 2, wherein each of said software products being previously encrypted on said at least one storage device by first encrypting each unsecured software product using a unique corresponding encryption key and subsequently decrypting the encrypted product using a unique phantom key, so that to decrypt each software product, each said full decryption key must correspond to said unique phantom key to encrypt said product and to said unique corresponding encryption key to decrypt the phantom encrypted product.

5. The system of claim 1, wherein each of said data corresponding to a respective software product includes at least one of the product manufacturer's name and trademarks, the location of said software product on said storage device, the platform type that will utilize said software product, and other software products relating thereto.

6. The system of claim 5, wherein said platform type is one of PC, Macintosh and UNIX based.

7. The system of claim 1, wherein said data file system further includes a plurality of universal files corresponding to one of a predetermined group or the entirety of said software products, wherein said processor, responsive to said application program, receives the data from the corresponding universal file.

8. The system of claim 7, wherein said data from said corresponding universal file includes verification to receive other necessary software products for said at least one storage device corresponding to the user selected software product.

9. The system of claim 2, wherein said application program includes an encrypted serial number stored therein which must be supplied to said server, with said data corresponding to a respective software product, to receive said partial decryption key, such that said server will not transmit said partial decryption key if any of said serial number, said data corresponding to a respective software product, and optionally a user password is determined to be invalid by said server.

10. The system of claim 1, wherein the decrypted selected software product is written to a storage medium.

11. The system of claim 10, wherein said processor, responsive to said application program, verifies that said storage medium includes a predetermined

data code, otherwise said decrypted software product is lost and not written to said storage medium.

12. The system of claim 11, wherein said storage medium is a floppy disk.

13. The system of claim 1, wherein each of said at least one storage device is a CD-Rom.

14. A method for retrieving a plurality of secured electronic information stored in at least one storage device, each being at least partially encrypted, and each of said plurality of secured electronic information being a software product, comprising the steps of:

selecting one of said software products for decryption through an application program stored in a user station, said user station having a processor responsive to said application program and to a separate data file system, said data file system including at least one database file, each comprising data corresponding to a respective one of said plurality of software products;

supplying said data regarding the corresponding selected product from said database files to said application program;

requesting, by said processor responsive to said application program, a decryption key from a remote network server based at least on said data from said database files;

selectively receiving said decryption key from said server to said processor responsive to said application program; and

decrypting said selected software product from said at least one storage device based on said decryption key.

15. The method of claim 14, wherein each said decryption key is a partial decryption key.

16. The method of claim 14, further comprising the step of processing the partial decryption key received from said server to generate a full decryption key, wherein said step of encrypting decrypts said selected software product based on said full decryption key.

17. The method of claim 16, further comprising the step of storing said full decryption key only until said selected software is decrypted.

18. The method of claim 16, wherein each said software product being previously encrypted on said at least one storage device by the steps of:

encrypting each unsecured software product using a unique corresponding encryption key, and

subsequently decrypting each encrypted product using a unique phantom key.

19. The method of claim 18, wherein said step of decrypting said selected software product comprises the steps of:

encrypting said selected software product based on said unique phantom key, and

decrypting the phantom encrypted product based on said unique corresponding encryption key,

wherein said phantom and corresponding encryption key is based on said generated full decryption key.

20. The method of claim 14, wherein each of said data corresponding to a respective software product includes at least one of the product manufacturer's name and trademarks, the location of said software product on said storage device, the platform type that will utilize said software product, and other software products relating thereto.

21. The method of claim 20, wherein said platform type is one of PC, Macintosh and UNIX based.

22. The method of claim 14, wherein said data file system further includes a plurality of universal files corresponding to one of a predetermined group or the entirety of said software products.

23. The method of claim 22, further comprising the step of selectively retrieving said predetermined group or said entirety of software products from said at least one storage device when said selected software product corresponds to one of said plurality of universal file.

24. The system of claim 16, wherein said step of requesting said decryption key from said server is further based on an encrypted serial number, stored in said application program, such that said server will not transmit said partial decryption key if any of said serial number, said data corresponding to a respective software product, and optionally a user password is determined to be invalid by said server.

25. The method of claim 14, further comprising the step of writing the decrypted selected software product to a storage medium.

26. The method of claim 25, further comprises the steps of:

verifying that said storage medium includes a predetermined data code;

destroying said decrypted software product without writing to said storage medium if such verification fails, and

writing said decrypted software product to said storage medium if such verification passes.

27. The method of claim 26, wherein said storage medium is a floppy disk.

28. The system of claim 14, wherein each of said at least one storage device is a CD-Rom.

5

FIG. 1

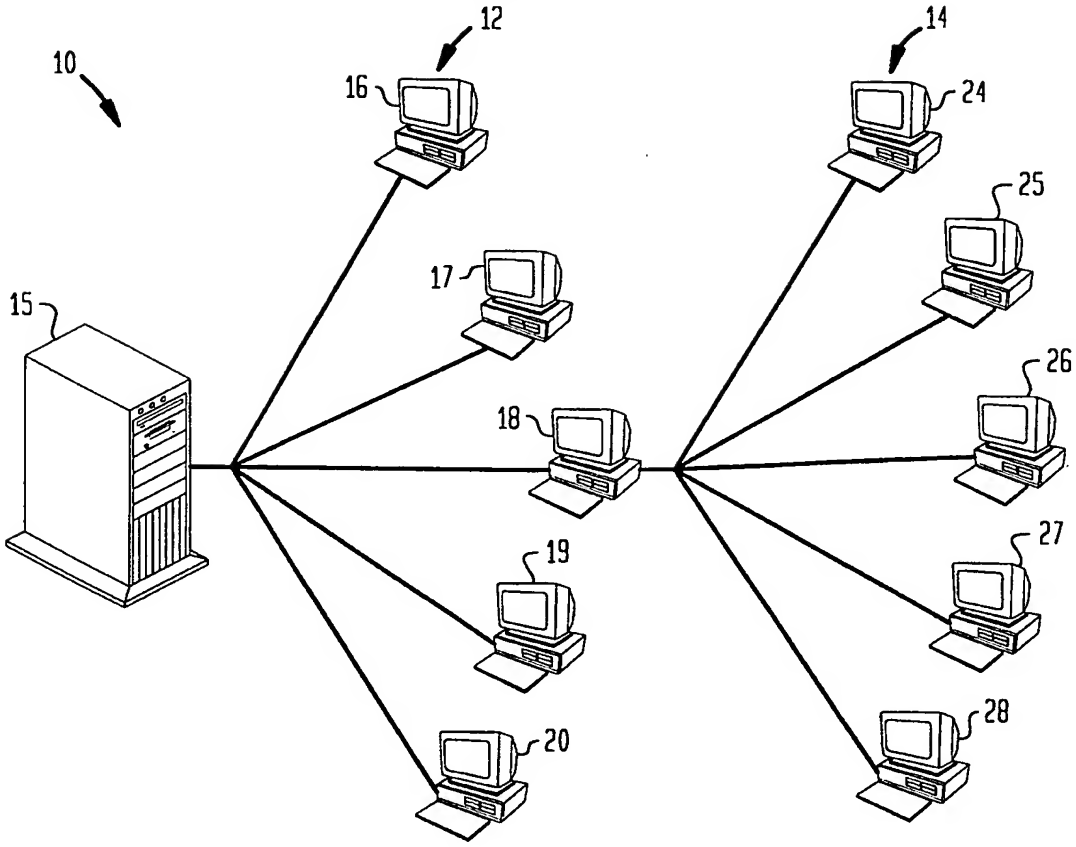

10
12
14
16
24
25
17
15
26
18
19
27
20
28

FIG. 2

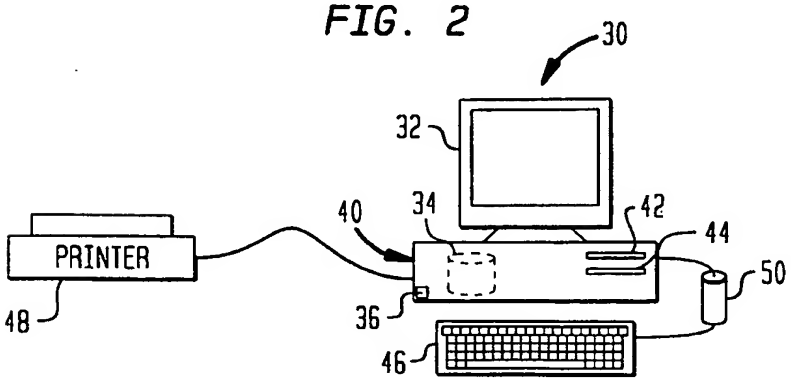

30
32
40
34
42
44
50
PRINTER
48
36
46

FIG. 3A

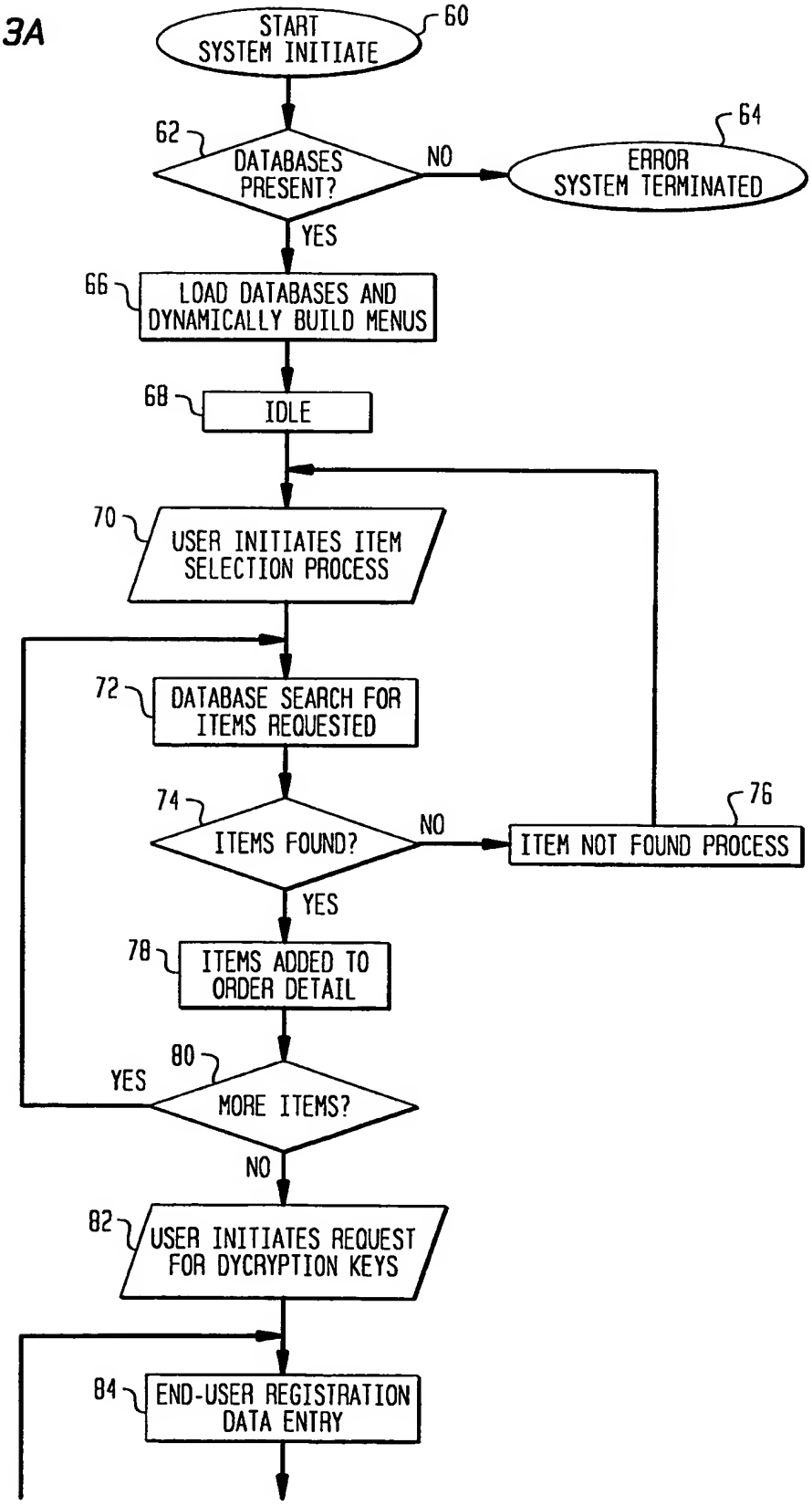

START SYSTEM INITIATE
60
62
DATABASES PRESENT?
NO
64
ERROR SYSTEM TERMINATED
YES
66
LOAD DATABASES AND DYNAMICALLY BUILD MENUS
68
IDLE
70
USER INITIATES ITEM SELECTION PROCESS
72
DATABASE SEARCH FOR ITEMS REQUESTED
74
ITEMS FOUND?
NO
76
ITEM NOT FOUND PROCESS
YES
78
ITEMS ADDED TO ORDER DETAIL
80
YES
MORE ITEMS?
NO
82
USER INITIATES REQUEST FOR DYCRYPTION KEYS
84
END-USER REGISTRATION DATA ENTRY

FIG. 3B

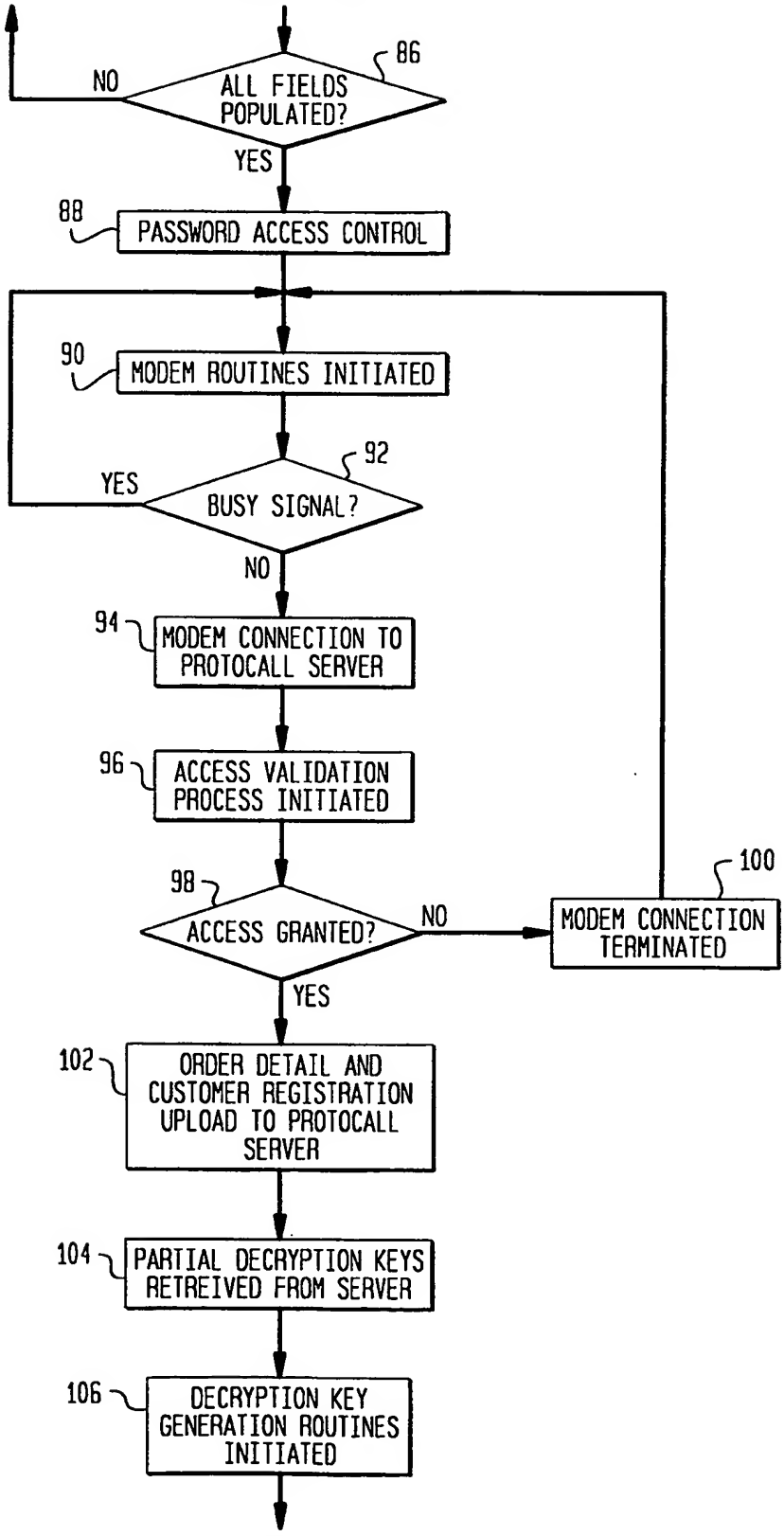

86
NO
ALL FIELDS POPULATED?
YES
88
PASSWORD ACCESS CONTROL
90
MODEM ROUTINES INITIATED
92
YES
BUSY SIGNAL?
NO
94
MODEM CONNECTION TO PROTOCALL SERVER
96
ACCESS VALIDATION PROCESS INITIATED
98
ACCESS GRANTED?
NO
100
MODEM CONNECTION TERMINATED
YES
102
ORDER DETAIL AND CUSTOMER REGISTRATION UPLOAD TO PROTOCALL SERVER
104
PARTIAL DECRYPTION KEYS RETREIVED FROM SERVER
106
DECRYPTION KEY GENERATION ROUTINES INITIATED

FIG. 3C

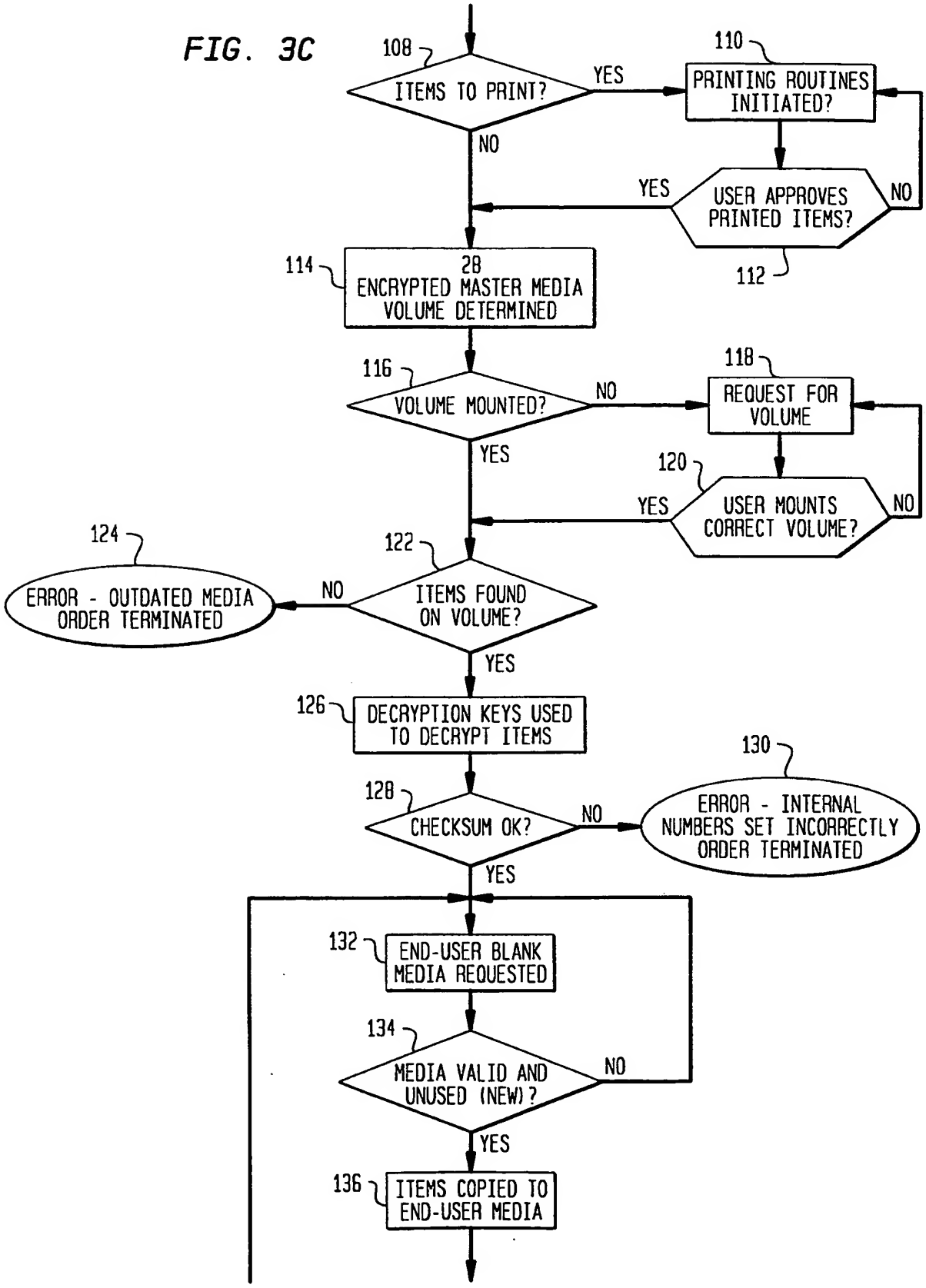

108
ITEMS TO PRINT?
YES
110
PRINTING ROUTINES INITIATED?
NO
YES
USER APPROVES PRINTED ITEMS?
NO
112
114
28
ENCRYPTED MASTER MEDIA VOLUME DETERMINED
116
VOLUME MOUNTED?
NO
118
REQUEST FOR VOLUME
YES
120
YES
USER MOUNTS CORRECT VOLUME?
NO
124
122
ERROR - OUTDATED MEDIA ORDER TERMINATED
NO
ITEMS FOUND ON VOLUME?
YES
126
DECRYPTION KEYS USED TO DECRYPT ITEMS
130
128
CHECKSUM OK?
NO
ERROR - INTERNAL NUMBERS SET INCORRECTLY ORDER TERMINATED
YES
132
END-USER BLANK MEDIA REQUESTED
134
MEDIA VALID AND UNUSED (NEW)?
NO
YES
136
ITEMS COPIED TO END-USER MEDIA

FIG. 3D

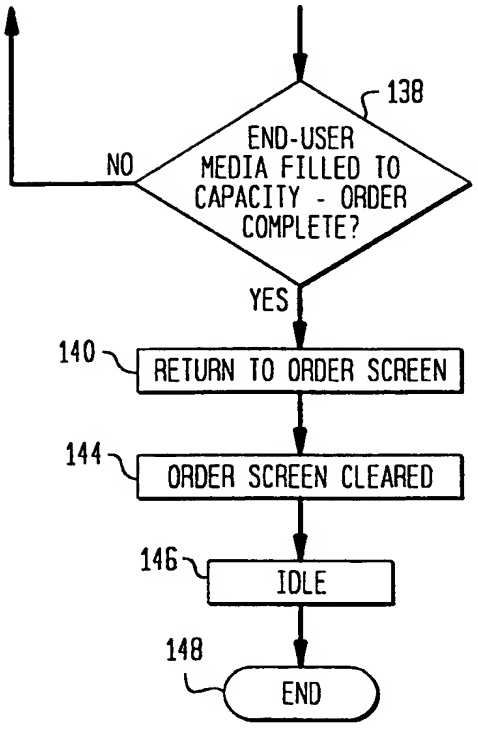

138
END-USER MEDIA FILLED TO CAPACITY - ORDER COMPLETE?
NO
YES
140
RETURN TO ORDER SCREEN
144
ORDER SCREEN CLEARED
146
IDLE
148
END

FIG. 4A

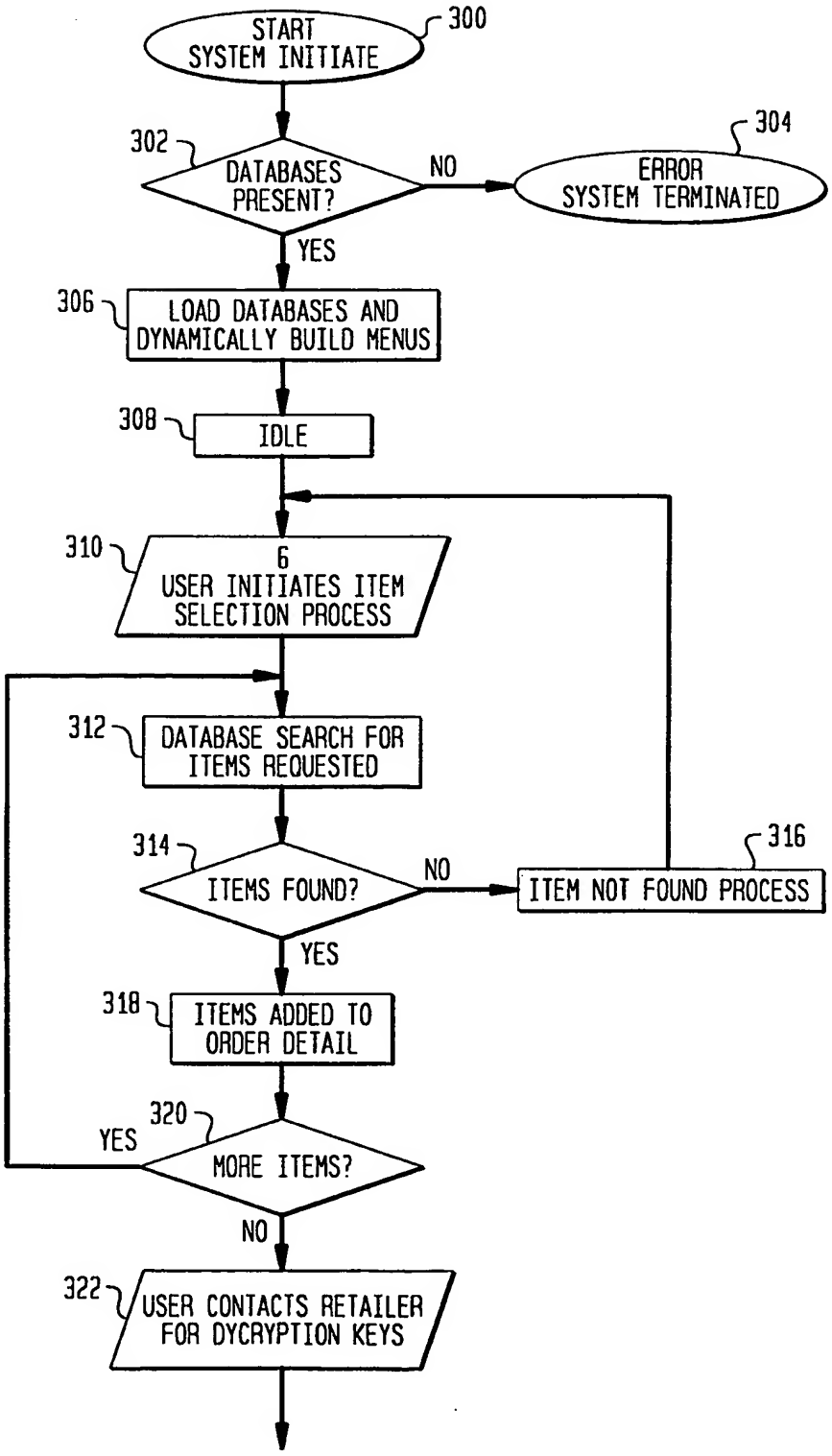

START SYSTEM INITIATE
300
302
DATABASES PRESENT?
NO
304
ERROR SYSTEM TERMINATED
YES
306
LOAD DATABASES AND DYNAMICALLY BUILD MENUS
308
IDLE
310
6
USER INITIATES ITEM SELECTION PROCESS
312
DATABASE SEARCH FOR ITEMS REQUESTED
314
ITEMS FOUND?
NO
316
ITEM NOT FOUND PROCESS
YES
318
ITEMS ADDED TO ORDER DETAIL
320
YES
MORE ITEMS?
NO
322
USER CONTACTS RETAILER FOR DYCRYPTION KEYS

FIG. 4B

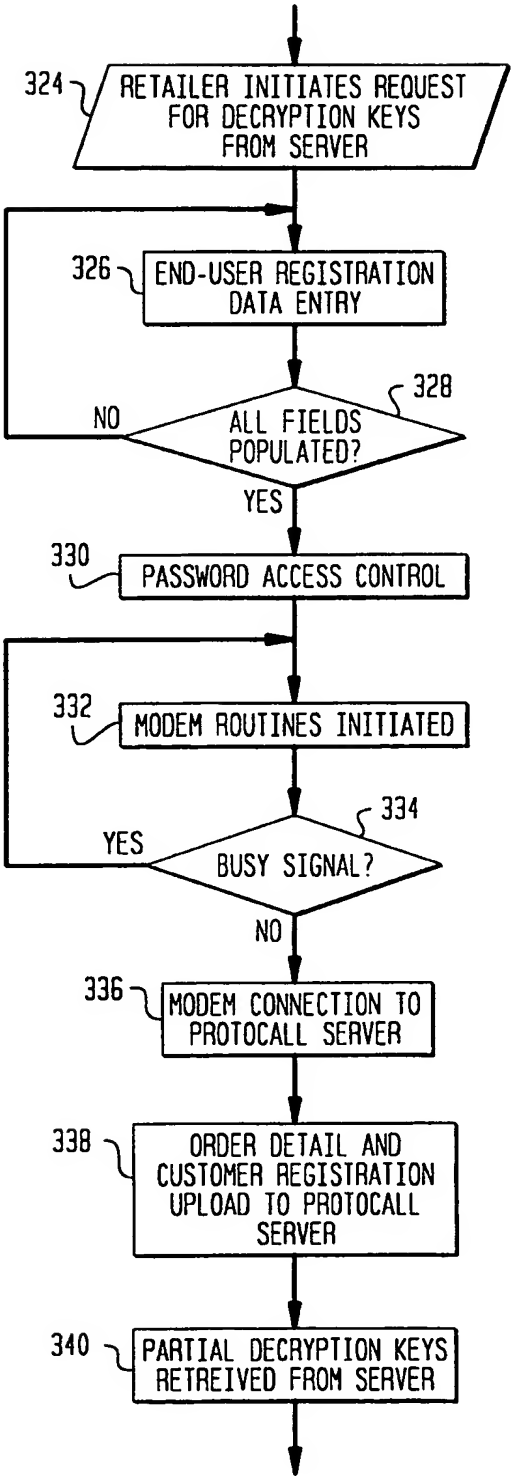

324
RETAILER INITIATES REQUEST FOR DECRYPTION KEYS FROM SERVER
326
END-USER REGISTRATION DATA ENTRY
328
ALL FIELDS POPULATED?
NO
YES
330
PASSWORD ACCESS CONTROL
332
MODEM ROUTINES INITIATED
334
BUSY SIGNAL?
YES
NO
336
MODEM CONNECTION TO PROTOCALL SERVER
338
ORDER DETAIL AND CUSTOMER REGISTRATION UPLOAD TO PROTOCALL SERVER
340
PARTIAL DECRYPTION KEYS RETREIVED FROM SERVER

FIG. 4C

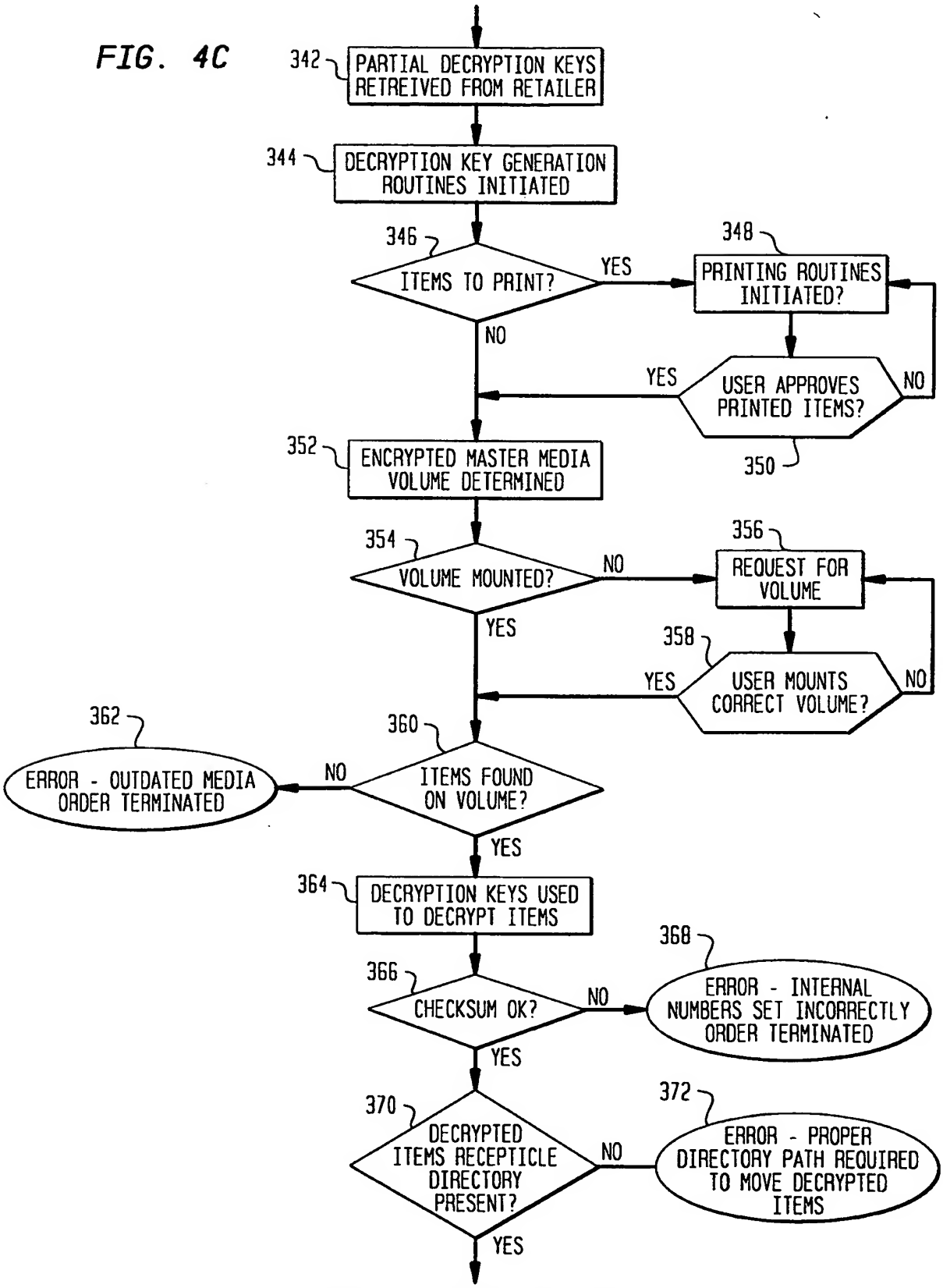

342
PARTIAL DECRYPTION KEYS RETREIVED FROM RETAILER
344
DECRYPTION KEY GENERATION ROUTINES INITIATED
346
ITEMS TO PRINT?
YES
348
PRINTING ROUTINES INITIATED?
NO
YES
USER APPROVES PRINTED ITEMS?
NO
350
352
ENCRYPTED MASTER MEDIA VOLUME DETERMINED
354
VOLUME MOUNTED?
NO
356
REQUEST FOR VOLUME
YES
358
USER MOUNTS CORRECT VOLUME?
YES
NO
362
ERROR - OUTDATED MEDIA ORDER TERMINATED
NO
360
ITEMS FOUND ON VOLUME?
YES
364
DECRYPTION KEYS USED TO DECRYPT ITEMS
368
ERROR - INTERNAL NUMBERS SET INCORRECTLY ORDER TERMINATED
366
CHECKSUM OK?
NO
YES
372
ERROR - PROPER DIRECTORY PATH REQUIRED TO MOVE DECRYPTED ITEMS
370
DECRYPTED ITEMS RECEPTICLE DIRECTORY PRESENT?
NO
YES

FIG. 4D

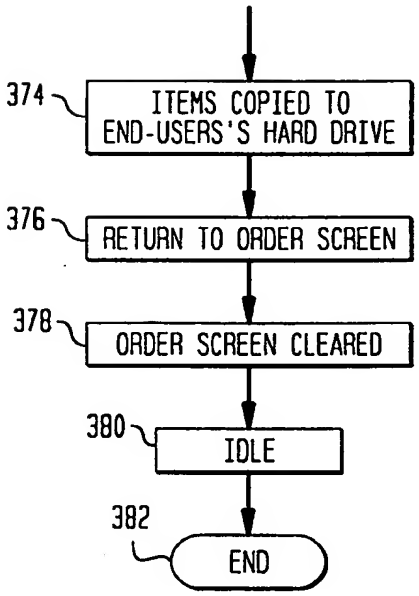

374
ITEMS COPIED TO END-USERS'S HARD DRIVE
376
RETURN TO ORDER SCREEN
378
ORDER SCREEN CLEARED
380
IDLE
382
END

FIG. 5A

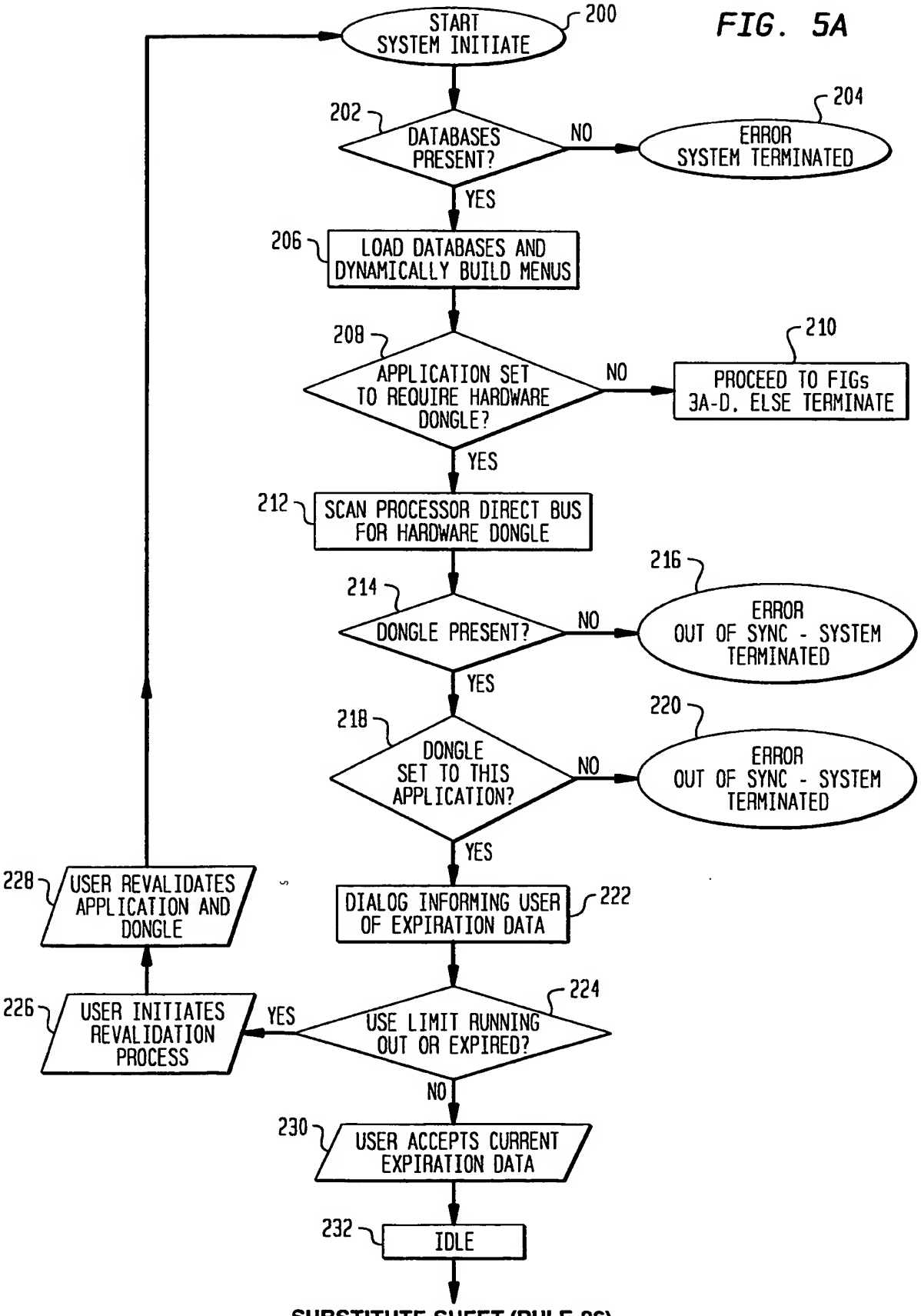

START SYSTEM INITIATE
200
DATABASES PRESENT?
202
NO
ERROR SYSTEM TERMINATED
204
YES
LOAD DATABASES AND DYNAMICALLY BUILD MENUS
206
APPLICATION SET TO REQUIRE HARDWARE DONGLE?
208
NO
PROCEED TO FIGs 3A-D. ELSE TERMINATE
210
YES
SCAN PROCESSOR DIRECT BUS FOR HARDWARE DONGLE
212
DONGLE PRESENT?
214
NO
ERROR OUT OF SYNC - SYSTEM TERMINATED
216
YES
DONGLE SET TO THIS APPLICATION?
218
NO
ERROR OUT OF SYNC - SYSTEM TERMINATED
220
YES
DIALOG INFORMING USER OF EXPIRATION DATA
222
USE LIMIT RUNNING OUT OR EXPIRED?
224
YES
USER INITIATES REVALIDATION PROCESS
226
USER REVALIDATES APPLICATION AND DONGLE
228
NO
USER ACCEPTS CURRENT EXPIRATION DATA
230
IDLE
232

FIG. 5B

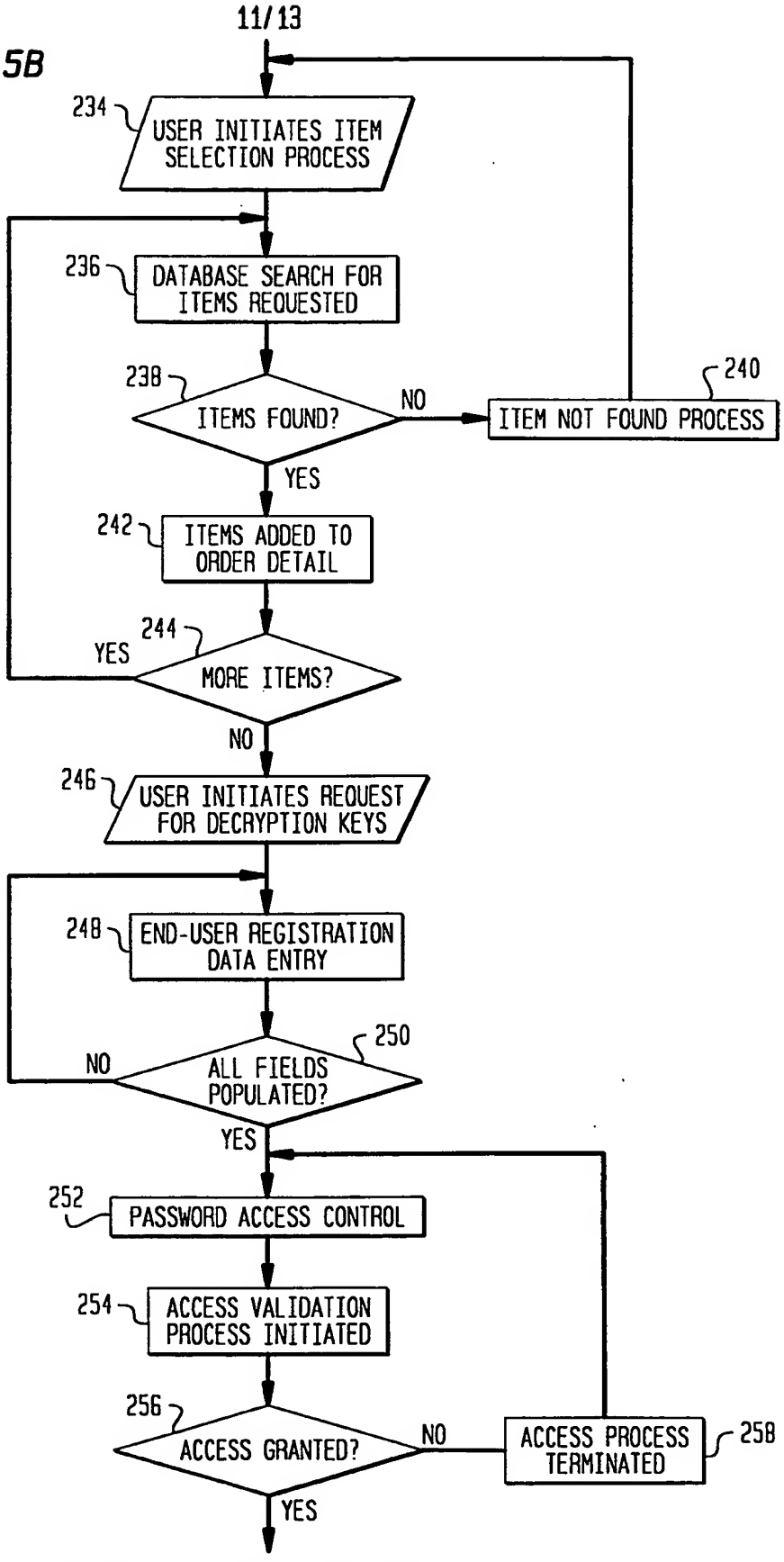

234
USER INITIATES ITEM SELECTION PROCESS
236
DATABASE SEARCH FOR ITEMS REQUESTED
238
ITEMS FOUND?
NO
240
ITEM NOT FOUND PROCESS
YES
242
ITEMS ADDED TO ORDER DETAIL
244
YES
MORE ITEMS?
NO
246
USER INITIATES REQUEST FOR DECRYPTION KEYS
248
END-USER REGISTRATION DATA ENTRY
250
NO
ALL FIELDS POPULATED?
YES
252
PASSWORD ACCESS CONTROL
254
ACCESS VALIDATION PROCESS INITIATED
256
ACCESS GRANTED?
NO
ACCESS PROCESS TERMINATED
258
YES

FIG. 5C

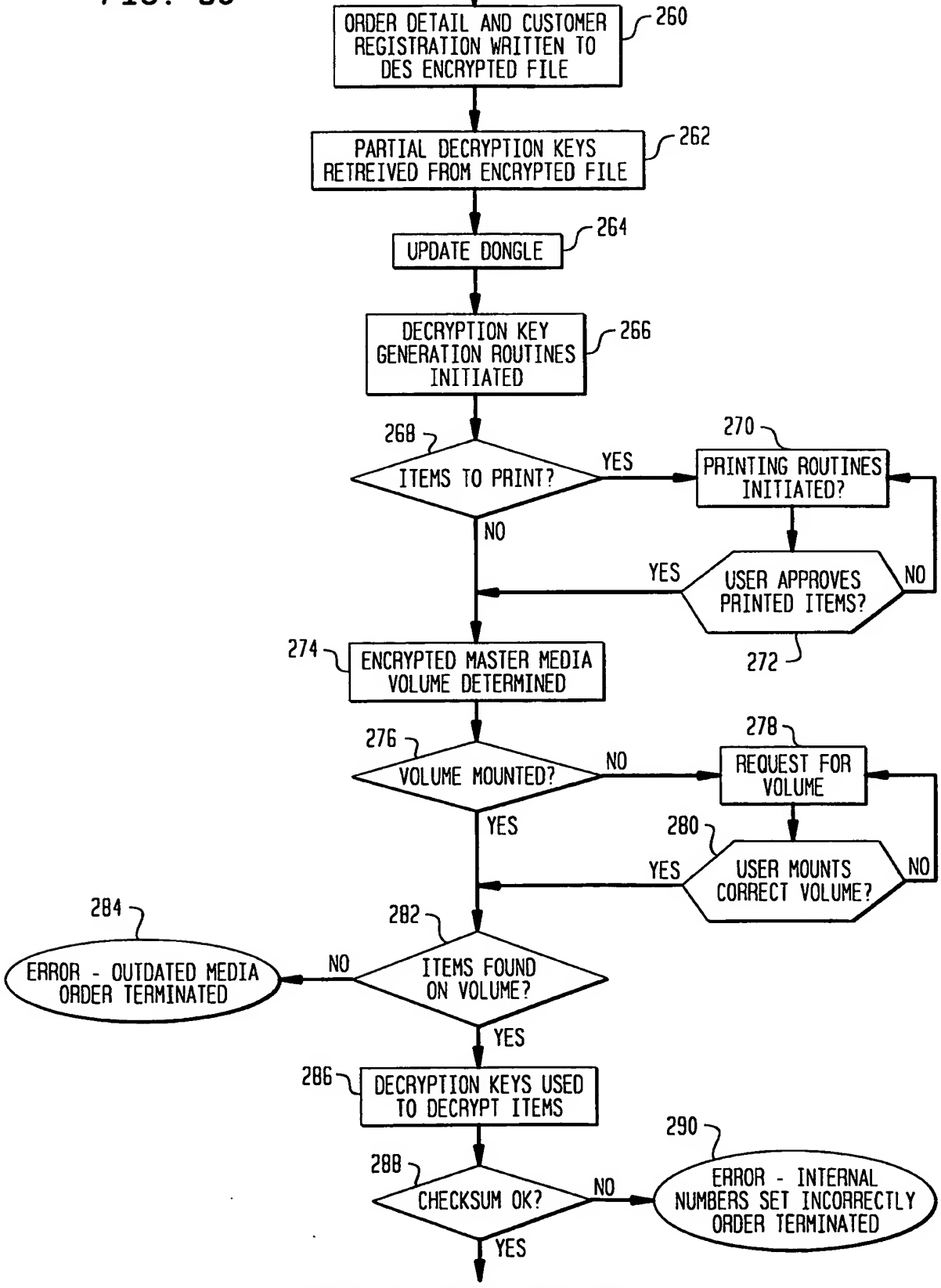
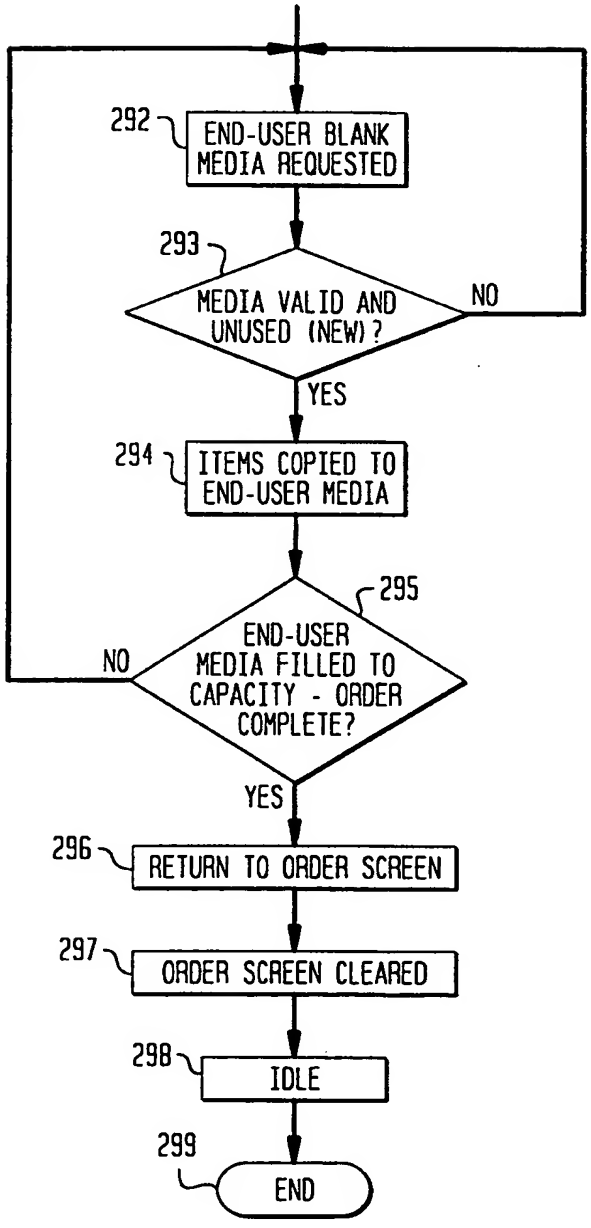

ORDER DETAIL AND CUSTOMER REGISTRATION WRITTEN TO DES ENCRYPTED FILE
260
PARTIAL DECRYPTION KEYS RETREIVED FROM ENCRYPTED FILE
262
UPDATE DONGLE
264
DECRYPTION KEY GENERATION ROUTINES INITIATED
266
268
ITEMS TO PRINT?
YES
NO
270
PRINTING ROUTINES INITIATED?
USER APPROVES PRINTED ITEMS?
YES
NO
272
274
ENCRYPTED MASTER MEDIA VOLUME DETERMINED
276
VOLUME MOUNTED?
NO
YES
278
REQUEST FOR VOLUME
280
USER MOUNTS CORRECT VOLUME?
YES
NO
282
ITEMS FOUND ON VOLUME?
NO
284
ERROR - OUTDATED MEDIA ORDER TERMINATED
YES
286
DECRYPTION KEYS USED TO DECRYPT ITEMS
288
CHECKSUM OK?
NO
290
ERROR - INTERNAL NUMBERS SET INCORRECTLY ORDER TERMINATED
YES

FIG. 5D


292
END-USER BLANK MEDIA REQUESTED
293
MEDIA VALID AND UNUSED (NEW)?
NO
YES
294
ITEMS COPIED TO END-USER MEDIA
295
END-USER MEDIA FILLED TO CAPACITY - ORDER COMPLETE?
NO
YES
296
RETURN TO ORDER SCREEN
297
ORDER SCREEN CLEARED
298
IDLE
299
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/18164

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/4, 21, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,548,645 A (ANANDA) 20 August 1996 Fig. 13	1-28
X	US 5,509,070 A (SCHULL) 16 April 1996 Fig. 1	1-28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 26 JANUARY 1998	Date of mailing of the international search report 17 MAR 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer for DAVID CAIN Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*